WHAT IS CLAIMED IS:

1. In a cryptographic device for performing a Data Encryption Standard (DES) type block cipher operation on a block of a plain text data bits under control of a set of cipher key bits including first storage means storing said block of data bits, first linear transformation means permuting said set of cipher bits, means connected to said first store means duplicating predetermined ones of the data bits of said block of data bits to produce an expanded block of data bits equal in number to the number of said permuted cipher key bits, means connected to said expansion means and said first linear transformation means carrying out a substitution transformation function in accordance with said expanded block of data bits and said permuted cipher key bits to produce a substitution set of bits equal to the number of bits in said block of data, the improvement comprising:

a second variable linear and cipher key dependent transformation means for providing a substantially increased level of encryption security compared to a standard DES device while retaining system compatability with the traditional DES cipher device whereby the combined transformation results in a product block cipher of said block of data bits with little or no increase in said encryption cycle time compared to a standard DES device.

2. The improved cryptographic device of Claim 1 additionally including logic gate means coupling said substitution means to said second transformation means for permuting said substitution set of bits and wherein said set of cipher key bits is substantially larger than a set of cipher key bits for a standard DES device.

3. The improved cryptographic device of Claim 1 wherein a fixed permutation function of said standard DES device is replaced by a time varying and cipher key dependent permutation.

4. The improved cryptographic device of Claim 3 wherein the improved device is selectively convertible for full compatability of a standard DES device and additionally including means for selectively setting predetermined bits of said set of cipher key bits to predetermined values to achieve compatability with said DES device.

5. The improved cryptographic device of Claim 2 wherein said logic gate means comprises an array of selectably coupled binary switches for generating time varying permutations of an output of said substitution transformation function which produces a substitution set of bits.

6. The improved cryptographic device of Claim 2 additionally including digital storage means for storing said larger set of cipher key bits and logic means for dividing said larger set of cipher key bits into a plurality of segments.

7. The improved cryptographic device of Claim 6 additionally including logic means for selectively generating a user designatable privacy code from one of said portions of said cipher key bits for providing individual user privacy.

8. A digital electronic process for ciphering/deciphering a group of data bits

under control of a set of cipher key bits wherein the set of cipher key bits is substantially larger than the length of the Data Encryption Standard (DES) cipher key and wherein an encryption/decryption cycle time is substantially equivalent to the cycle time of a standard DES device, the process comprising the steps of:

storing said group of data bits in a first digital storage memory,

storing said set of cipher key bits in a second digital storage memory,

separating said stored cipher key bits into at least a first segment and a second segment,

linearly transforming said first set of cipher key bits into a plurality of transformed cipher key bits,

performing a plurality of different substitution transformation functions using said transformed cipher key bits on said group of data bits, and

performing a second time varying transformation of said substitution set of bits under control of said second segment of said cipher key bit section whereby the combined transformations generate a product block cipher of said block of data bits.

9.The cipher/decipher process of Claim 8 including an additional step of selectively modifying portions of said first or said second segments of said stored cipher key bits to selectively render the process fully compatible with a standard encryption/decryption process of a standard DES device.

10. An improved Data Encryption Standard (DES) device for performing a

Product block cipher operation on a block of data bits under control of a set of cipher key bits wherein said set of cipher key bits is substantially larger than a typical cipher key set of a standard DES device, said improved DES device comprising:

a digital memory for storing said block of data bits,

a key bit storage register for storing said set of cipher key bits and for dividing said key bits into at least two segments,

a first linear transformation logic gate array for permuting said bits of said first segment of said cipher key bits,

a storage memory register for grouping said permuted cipher key bits into a plurality of permuted cipher key bits,

a binary logic gate array coupled to said storage memory register for producing an expanded block of data bits equal in number to the number of permuted cipher key bits,

a second binary gate array responsive to said plurality of permuted data bit segments and to said plurality of permuted cipher key bit segments for executing different substitution transformation functions to generate a substitution set of data bits equal in number to the number of bits in said block of data bits, and

a second time variable, key dependent linear transformation logic gate array of binary switches controlled by said second segment of said cipher key bits and coupled to said first substitution transformation gate array whereby the combined transformations result in a product cipher of said block of data bits without substantially increasing the cipher cycle time compared to a standard DES device.

11. The improved DES type block cipher device of Claim 10 additionally including

an optional DES compatability switch for selectively predetermining a value for ones of the bits of the cipher key bit register to ensure compatability with a standard DES device.

12. The improved DES type cipher device additionally including an operator selectable switch for activating a means of generating a unique user privacy code from said cipher key bits for providing individual users with a unique privacy function.